Data Security and Cyber Threat Update

Jimmy Buddenberg

1) In a ransomware attack does paying result in getting your data more than not? How do you guarantee payment will get your organizations data back?

   You can think of the ransomware industry as a business. If organizations never recovered their data after a ransomware attack the news would spread and everyone would be reluctant to pay. So, in most instances, paying the ransom does result in organizations being able to recover their data. That being said, you are dealing with criminals, so you always run the risk that they will take your money and not assist with recovering your information. It would be tough to receive any guarantees that you will be able to recover your data.

2) How do you know whether or not you are using VPN using the split tunneling method?

   In order to determine if you are using a VPN with split tunneling enabled you will need to use a technical command called tracert (stands for trace route). You will need to open a command prompt on your Windows computer and once at the prompt type in tracert 8.8.8.8 (this is a Google DNS server). VPN networks using split tunneling will display a trace that leads directly to their Internet provider (see below). If a VPN network is not configured for split tunneling there will be several additional hops beginning at line 2 (highlighted) that will demonstrate the traffic being routed through the VPN concentrator at your organization.

```
C:\Users\brian.kirk>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    4 ms    3 ms    4 ms  testwifi.here [192.168.86.1]
  2    4 ms    4 ms    4 ms  dtr03ssvlsc-tge-0-2-0-5.ssvl.sc.charter.com [96.34.67.216]
  3   20 ms   15 ms   15 ms  dtr01ssvlsc-tge-0-2-0-5.ssvl.sc.charter.com [96.34.67.217]
  4   19 ms   16 ms   17 ms  096-034-095-153.biz.spectrum.com [96.34.95.153]
  5   16 ms   16 ms   15 ms  crr01gnvlsc-bue-300.gnvl.sc.charter.com [96.34.93.199]
  6   18 ms   19 ms   17 ms  crr12gnvlsc-tge-0-1-0-1.gnvl.sc.charter.com [96.34.92.62]
  7   20 ms   22 ms   21 ms  bbr01spbgsc-bue-4.spbg.sc.charter.com [96.34.2.50]
  8   22 ms   22 ms   22 ms  bbr02slidla-tge-0-1-0-4.slid.la.charter.com [96.34.0.133]
  9   27 ms   41 ms   21 ms  bbr02atlnga-tge-0-2-0-0.atln.ga.charter.com [96.34.3.111]
 10   21 ms   20 ms   20 ms  74.125.51.142
 11   24 ms   25 ms   20 ms  108.170.225.164
 12   22 ms   22 ms   22 ms  108.170.225.117
 13   21 ms   21 ms   18 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\brian.kirk>
```

3) What percent of these criminals actually get caught?

   No one knows an accurate number to this question because most cybercrimes are not reported. Additionally, most criminals that are caught are never prosecuted. Finally, as most criminals operate outside the United States it makes it even more difficult to obtain an indictment. One of the reasons cybercrime is so prevalent is because it's extremely difficult to get caught and prosecuted.

4) Can we get his 13 recommendations document?

   Included

5) Do you recommend that capabilities be made to eliminate inserting flash drives into computers?

   Some organizations, such as banks, don't require the use of removable media on individual workstations. I would recommend you block the ability for flash drives to be used in your environment if they are not required.

6) How many days of backups is recommended? How often would you recommend an incremental vs full back up?

   Determining a company's backup rotation is dependent on their business model and how quickly they need to recover operations. In order to properly answer this question we would need to understand the type of business and the impact of downtime. Many companies do full backups on the weekends and incremental every day, however, some organizations perform full backups every night as they want to recover quickly in the event of an outage or cyber-attack. A company should have offline copies of full backups (either tape or cloud).

7) If a company pays the money to get their data back from the attacker, are there cases where the attackers keep copies of the company's data and still uses it even after they have been paid to return it? How is a company sure their data won't be used after they pay to get it back?

   There are no guarantees that you can trust criminals. Recent ransomware attacks have included a data exfiltration component so that attackers can also threaten to release the information obtained if the ransom is not paid. No one knows if the attackers truly destroy the data obtained if the ransom is paid.